UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,264	09/16/2003	Dirk Wertenbruch	50325-0778	3449

29989 7590 09/10/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
09/10/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DIRK WERTENBRUCH and PETER FALK

Appeal 2009-006319
Application 10/664,264[1]
Technology Center 2400

Before JOHN A. JEFFERY, JAY P. LUCAS, and JAMES R. HUGHES, *Administrative Patent Judges.*

HUGHES, *Administrative Patent Judge.*

DECISION ON APPEAL[2]

---

[1] Application filed September 16, 2003. The real party in interest is Cisco Systems, Inc. (App. Br. 1.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

The Appellants appeal from the Examiner's rejection of claims 1-41 under authority of 35 U.S.C. § 134(a). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellants' Invention

Appellants invented a method and apparatus for identifying and configuring a network device. (Spec. 8, ¶¶ [0024]-[0025].)[3]

Representative Claim

Independent claim 1 further illustrates the invention. It read as follows:

> 1. A method of authenticating a network device, comprising the computer-implemented steps of:
>
> determining that a network link that uses a primary signaling technology and a secondary signaling technology is coupled to the network device;
>
> obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology;
>
> establishing the unique link identifier as a unique device identifier; and
>
> authenticating the network device to a service provider by communicating the unique device identifier to the service

[3] We refer to Appellants' Specification ("Spec."); Appeal Brief ("App. Br.") filed March 12, 2008; and Reply Brief ("Reply Br.") filed July 3, 2008. We also refer to the Examiner's Answer ("Ans.") mailed May 22, 2008; the Advisory Action ("Adv. Action") mailed October 19, 2007; and the Final Office Action ("Fin. Rej.") mailed August 6, 2007.

provider over the network link using the primary signaling technology.

References

The Examiner relies on the following references as evidence of unpatentability:

Li	US 6,012,088	Jan. 4, 2000
Fijolek	US 6,351,773 B1	Feb. 26, 2002

Rejection on Appeal

The Examiner rejects claims 1-41 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Li and Fijolek.

ISSUES

Based on our review of the administrative record, Appellants' contentions, and the Examiner's findings and conclusions, the pivotal issues before us are as follows:

1. Does the Examiner err in finding the Li and Fijolek references would have collectively taught or suggested obtaining, using a secondary signaling technology, a unique link identifier that is associated with a network link using a primary and the secondary signaling technology?

2. Does the Examiner err in finding the Li and Fijolek references would have collectively taught or suggested obtaining, using an ISDN line, an ISDN telephone number uniquely associated with the ISDN line?

FINDINGS OF FACT (FF)

Li Reference

1. Li describes a system and device for automatically configuring a computing system for communication with a communications network such as the Internet. (Abst.; col. 1, ll. 13-17; col. 3, ll. 24-30.) Li's Internet access device automatically configures a customer's computer system to access the Internet by connecting the customer's system to a configuration server of an Internet Service Provider (ISP), downloading the desired configuration information, and configuring itself for the customer's system to access the Internet at the customer's desired level of service. (Col. 3, ll. 39-61; col. 11, l. 54 to col. 12, l. 27.)

2. Li's Internet access device initially connects to the Internet through an ISP to access the ISP's configuration server. The connection utilizes a standard analog telephone line and a modem, which acts as a single host computer using a dynamic Internet Protocol (IP) address as its address. (Col. 3, ll. 46-49, 54-57; col. 11, ll. 18-26, col. 11, l. 56 to col. 12, l. 18; col. 12, ll. 38-43; 49-56; figs.8 & 11a.) Once connected to the ISP, the Internet access device performs the automatic configuration process. The Internet access device establishes a Point to Point Protocol (PPP) connection with a Network Access Server (NAS) of the ISP, which "involves password negotiations, exchange of addresses, and other standard handshaking" (col. 13, ll. 3-4). (Col. 12, ll. 14-27, 38-48, 66 to col. 13, l. 4; fig.11a.) Next, the Internet access device provides the customer's registration ID to the ISP, which decodes the registration ID into an IP address for the configuration server and a unique customer account ID. (Col. 13, ll. 11-28; *see* col. 10, ll. 26-65.) The ISP provides the Internet access device with access to the

configuration server utilizing the decoded IP address. (Col. 13, ll. 29-48; figs.8 & 11a.) The Internet access device then requests from the configuration server particular configuration information (a configuration file or record) for the customer's system utilizing the customer's account ID, and downloads the information utilizing the temporary (dynamic) IP address for the Internet access device. The Internet access device then configures itself. (Col. 13, l. 60 to col 14, l. 12; col 14, ll. 20-33; fig.11b; *see* col. 9, l. 26 to col. 10, l. 24; col. 14, l. 50 to col. 15, l. 9; col. 15, ll. 17-44; fig.12.) Once Li's Internet access device is properly configured, it acts as a router for connecting to the Internet utilizing a static (permanent) IP address (or range of IP addresses) and more complex, higher speed connections such as ISDN or frame relay. (Col. 3, ll. 57-61; col. 11, ll. 27-45; col. 14, ll. 41-49; fig.9.)

3. Li describes utilizing an ISDN connection or a dial-up ISDN line to access the Internet. (Col. 2, ll. 32-36; col. 3, ll. 49-53; col. 9, ll. 34-37.) Li further describes that the configuration information for an ISDN connection includes the customer's ISDN directory number and a Service Profile Identifier (SPID). (Col. 15, ll. 38-44.)

Fijolek Reference

4. Fijolek describes a data-over-cable system including a Cable Modem (CM), a Telephone Remote Access Concentrator (TRAC), a Cable Modem Termination System (CMTS) and a data network. The CM connects to the CMTS through a downstream or (alternatively) bi-directional cable network. In a system utilizing telephony return, the CM connects to the TRAC utilizing an upstream connection to a Public Switched Telephone Network (PSTN). The CMTS and TRAC connect to the data network through network system interfaces. (Col. 5, l. 1 to col. 6, ll. 47; fig.1.)

While Fijolek describes upstream data communications utilizing the PSTN and TRAC (telephony return), as well as upstream communications utilizing the cable network and CMTS, these are alternative embodiments (i.e., mutually exclusive). (Col. 5, ll. 11-20; col. 6, ll. 45-47; col. 13, ll. 21-27.)

5. Fijolek describes a detailed method for establishing data communication in its data-over-cable system between the CM and data network utilizing upstream communications from the CM through the PSTN and TRAC to the data network, and from the data network through the CMTS and cable network to the CM. (Col. 11, l. 54 to col. 13, l. 27; col. 15, l. 19 to col. 18, l. 67; figs.1, 2, 7A, 7B, 8 & 9.) Fijolek's CM dials into the TRAC and establishing a telephony PPP connection. The CM negotiates an IP address with the TRAC for sending IP data packets (responses) to the data network through the TRAC via the PPP. Then, the CM creates a virtual data connection that allows the CM to receive data from data network through the CMTS and cable network, and to send return data to data network through the PSTN and TRAC. The CM creates the virtual connection using the Dynamic Host Configuration Protocol (DHCP) layer (figure 2) to discover network host interfaces available on the CMTS (the DHCP discovery process). Fijolek's Table 3 describes the exemplary data path (virtual connection) in the system. An IP message from the data network for the CM passes through the CMTS network interface to the CMTS. The CMTS encodes the message in a cable data frame and passes it to the Medium Access Control (MAC) layer which transmits it to the CM through the cable network. The CM recognizes the encoded message in MAC layer of the cable data frame and sends a response message in a PPP frame through the PSTN to the TRAC. The TRAC decodes the return message and forwards it

through the TRAC network interface to the data network. (Col. 13, ll. 28-40, tbl.3.)

6. Fijolek (*see* fig.9) also describes a detailed method for performing DHCP discovery in a system with telephony return (utilizing upstream communications from the CM through the PSTN and TRAC). (Col. 11, l. 54 to col. 13, l. 27; col. 15, l. 19 to col. 18, l. 67; figs.1, 2, 7A, 7B, 8 & 9.) Fijolek's CM establishes an IP link to the TRAC using PPP, and then initiates the DHCP discovery process by communicating with the CMTS via the DHCP layer in order to complete the virtual IP connection with the data network. The CM generates and sends a DHCP discover message to the TRAC (via the PSTN). The fields of the DHCP discover message include various addresses (CIADDR (client IP address - the CM's previously assigned IP address, if available), GIADDR (gateway IP address - the downstream channel IP address of the CMTS), and CHADDR (client hardware address - the CM's 48-bit MAC address)). The TRAC broadcasts the DHCP discover message to DHCP proxies within the TRAC's local network, which forward the DHCP discover message to the DHCP servers associated with network host interfaces available to the CMTS. The DHCP servers generate DHCP offer messages in response to the DHCP discover message, and send the offer messages to the CMTS using the downstream channel IP address of the CMTS (GIADDR). The fields of the DHCP offer messages include configuration parameters and various addresses (YIADDR (client ("your") IP address - the address of the network host interface of the CMTS used to receive data from the data network and send the data to the CM (i.e., the CM's IP address)) and CHADDR (the CM's MAC address)). (Col. 15, l. 39 to col. 17, l. 40.) The CMTS forwards the DHCP offer

messages to the CM via the cable network utilizing the MAC layer address (CHADDR). The CM receives the DHCP offer messages, selects one of the messages (an offer for IP service from one of the network host interfaces (IP interfaces) available on the CMTS), and establishes (completes) the virtual IP connection by acknowledging the selected network host interface with a return DHCP message to the IP address of the selected network host interface included in the DHCP offer message. (Col. 17, l. 41 to col. 18, l. 67.)

7. Fijolek describes the CM connected through the PSTN and the TRAC for upstream communication with the data network. The PSTN connection may comprise a standard telephone line connection, an Integrated Services Digital Network (ISDN) connection, an Asymmetric Digital Subscriber Line (ADSL) connection, or other telephony connection. (Col. 5, ll. 52-55; see col. 5, ll. 43-57; col. 7, ll. 36-54.)

8. Fijolek describes providing restricted access to subscription services for network devices (e.g., the CM), in the data-over-cable system. The CM makes a connection request to the CMTS, and the CMTS checks its associated databases for information about the CM. (Col. 31, l. 8 to col. 32, l. 11.) The CM information may include "a subscription account number, a calling party number, a MAC 44 address, or other information." (Col. 32, ll. 7-11.) Alternately, a Remote Authentication Dial In User Server (RADIUS) server may be used to check for information about the CM. Fijolek explains that RADIUS servers are well known in the art for receiving and processing user connection requests, authenticating a user, and providing configuration information necessary for a client to deliver service to a user, and the

RADIUS server may be associated with either the TRAC or the CMTS. (Col. 32, ll. 16-31.)

9. Fijolek describes changing a restricted network connection to an unrestricted connection between the CM and the data-over-cable system. Specifically, the CMTS collects (obtains) information from the CM that uniquely identifies the CM on the data-over-cable system, and the CMTS stores the information in a database. (Col. 33, l. 29 to col. 34, l. 10.) The information may include "account verification information, such as a credit card number and corresponding approval/denial information, local connection information, such as area code or other local numbers, a class-of-service or a quality-of-service for connections to the data-over-cable system, device configuration information, a MAC 44 address, and other information." (Col. 34, ll. 4-10.)

ANALYSIS

Issue 1: Rejection of Claims 1-9 and 14-41 under § 103

Appellants contend that the combination of the Li and Fijolek references does not disclose, teach, or suggest "obtaining, using the secondary signaling technology, a unique link identifier that is associated with the network link using the secondary signaling technology," as recited in Claim 1. (App. Br. 7-8; Reply Br. 2-4.) The Examiner, on the other hand, finds that the Li and Fijolek references teach the disputed features. (Ans. 3, 7-9; Fin. Rej. 2-4.) Specifically, the Examiner finds in the Final Office Action that: "Li teaches two signaling technologies" – a standard telephone line and an ISDN connection – and a user entering "a local telephone number;" and that the Fijolek reference "teaches that the unique identifier

can be obtained from a secondary signaling technology, such as from a database." (Fin. Rej. 3.) The Examiner also finds that Li does not explicitly teach the "obtaining" step, but Fijolek "teaches that a parameter could be the calling party's phone number." (Fin. Rej. 4.) The Examiner additionally finds that "Fijolek teaches that multiple secondary signaling methods can be used for communication," and that the "secondary signaling means can be wireless, satellite, or a connection with other technologies to send data upstream[, and] [t]he 'link identifier' is know to be attached to any message sent using the signaling technology." (Adv. Action 2.)

In the Answer, the Examiner reiterates the previous findings (Ans. 3, 7), and also finds that "[a] unique link identifier is interpreted to be any of the following: registration identification number, as described in Li or a subscription account number, a calling party number, a MAC address as described in Fijolek." (Ans. 7.) The Examiner additionally finds Fijolek teaches that "data can be sent from customer premise equipment over cable networks via cable as well as secondary signaling method such as a telephony network, wireless connection, satellite, or connection via other technologies" (Ans. 8); and "the Cable Modem Termination System (CMTS) checks one or more databases for information . . . . includ[ing] a subscription account number, a calling party number, a MAC address, or other information . . . . [which] is obviously a 'unique identifier' . . . . included in the connection request, i.e. obtained using a secondary signaling technology" (Ans. 8-9).

We agree with Appellants that the Li and Fijolek references do not teach the disputed "obtaining" step of claim 1 for essentially the reasons espoused by Appellants. The dispute before us hinges on the disagreement

of Examiner and Appellants as to what constitutes "obtaining," "a unique link identifier," "associated with the network link," "using the secondary signaling technology," and the interpretation of the terms in the disputed feature is critical to resolving this dispute. We broadly but reasonably (*see In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004)) construe Appellants' disputed claim limitation to mean gaining possession of (obtaining) a unique identifier for a network connection (connecting element or link) that utilizes two different signaling technologies – a primary and a secondary signaling technology – using the secondary signaling technology to obtain the unique identifier for an undetermined entity.

As detailed in the Findings of Fact section *supra*, Li describes two signaling technologies – analog telephone and ISDN. (FF 1-3.) We, however, do not find Li to describe using these technologies in the same connection. Rather, Li describes using a different more complex connection (ISDN or frame relay) after the system is configured. (FF 2-3.) Even if we interpret these separate connections as a link using primary (ISDN) and secondary (analog telephone) signaling technologies, Li still does not explicitly describe transferring a unique identifier for the link, either from the Internet access device to the ISP or from the ISP to the Internet access device – i.e., the ISP obtaining the identifier or the Internet access device obtaining the identifier.

We agree with Appellants that Li's telephone number cannot represent a unique identifier for the link. Li's registration number also does not represent a unique identifier for the link. The registration number represents the customer/user and/or the user equipment, not the link – Li uses the decoded customer ID to retrieve the Internet access device

configuration, but does not describe any relationship between the customer ID and the telephone connection (secondary signaling technology). (FF 2.)

Although Li describes negotiating, sending, and receiving IP addresses (dynamic and static IP addresses) for the Internet access device (FF 2), Li does not provide a detailed explanation of negotiating, sending, and receiving the IP addresses. Neither the Examiner nor Appellants address this aspect of Li.

Fijolek describes a data-over-cable system that provides restricted and unrestricted network connections between a CM and a data network. (FF 4-6, 8-9.) Fijolek describes the data-over-cable system and its basic operation (*see* FF 4-6) separately from the system's functionality of providing restricted/unrestricted access (*see* FF 8-9). The Examiner addresses Fijolek's functionality of providing restricted access – finding Fijolek's CMTS checks databases for information concerning a particular CM including a subscription account number, a calling party number, and/or a MAC address, which the Examiner finds to be a "unique identifier." The Examiner, however, sidesteps any detailed discussion of the data-over-cable system and its operation – simply finding that Fijolek teaches secondary signaling technologies to send data upstream, that the data may include messages or connection requests, and that an identifier for the link may be included in the messages or connection requests.

Although we understand Fijolek to describe transferring messages including identifiers, Fijolek does not transfer the identifiers for a link that utilizes both primary and secondary signaling technologies using the secondary signaling technology. Fijolek transfers (sends and receives) messages (DHCP discover and DHCP offer messages) between the CM and

CMTS. (FF 4-6.) The DHCP discover messages contain information uniquely identifying the CM (a MAC address of the CM), and the DHCP offer messages contain information uniquely identifying the CM (the IP address for the CM and the CM's MAC address). (FF 6.) Fijolek also describes the CMTS checking databases for information identifying the CM – such as a MAC address – and the CM providing identifying information to the CMTS – such as a MAC address. (FF 8-9.) Fijolek, however, also describes two separate and distinct connections or links between the CM and the network (CMTS, TRAC, and data network) – an upstream telephone (PSTN) connection and a downstream cable network connection. Consequently, Fijolek does not describe a link using both primary and secondary signaling technologies. Thus, Fijolek also does not teach obtaining a unique identifier for a network link that utilizes both a primary and a secondary signaling technology using the secondary signaling technology.

The Examiner, in combining Li and Fijolek, merely states that:

> It would have been obvious to one of ordinary skill in the art at the time of a method for automatic configuration for [I]nternet access devices taught in [Li] to include a means utilize the number of the customer premises as a configuration parameter. One of ordinary skill in the art would have been motivated to perform such a modification to protect the access to a network [(See Fijolek column] 2, lines 53 et seq.).

(Fin. Rej. 4.) The Examiner fails to explain how an ordinarily skilled artisan would have understood Li's and Fijolek's separate network links to be a single network link utilizing both primary and secondary signaling technologies; or how or why an ordinarily skilled artisan would have utilized Fijolek's messages including identifiers in Li's configuration system.

Thus, we are constrained by the record before us to find that neither Li, nor does Fijolek individually disclose, nor does the combination teach or suggest the disputed feature of obtaining a unique identifier for a network link that utilizes both a primary and a secondary signaling technology using the secondary signaling technology. The Examiner has failed to set forth a prima facie obviousness rejection. It follows that Appellants have persuaded us to find error in the Examiner's obviousness rejection of Appellants' independent claim 1.

Appellants' independent claims 14, 15, 24, and 33 each include a limitation similar in scope to the disputed limitation of claim 1. It follows, for the reasons discussed *supra*, that the Li and Fijolek references do not render obvious Appellants' independent claims 14, 15, 24, and 33. Appellants' dependent claims 2-9 (depend on claim 1), 16-23 (depend on claim 15), 25-32 (depend on claim 24), and 34-41 (depend on claim 33) depend on their respective base independent claims. Therefore, based on the record before us, we find that the Examiner err in finding the Li and Fijolek references would have collectively taught or suggested obtaining, using a secondary signaling technology, a unique link identifier that is associated with a network link using a primary and the secondary signaling technology, as recited in Appellants' claims 1-9 and 14-41. Accordingly, we reverse the Examiner's obviousness rejection of claims 1-9 and 14-41.

Issue 2: Rejection of Claims 10-13 under § 103

Based on the record before us, we find also find error in the Examiner's obviousness rejection of Appellants' independent claim 10 which calls for, in pertinent part, "an ISDN line that supports ADSL over ISDN" and "obtaining, using the ISDN line, an ISDN telephone number

uniquely associated with the ISDN line" (claim 10). Although we agree with the Examiner that both Li (FF 2-3) and Fijolek (FF 7) teach using ISDN and ADSL signaling technologies (*see* Ans. 5, 9-10), neither Li, nor Fijolek provide an explicit description of ADSL over ISDN. Neither the Examiner, nor Appellants address this deficiency of the cited references. We decline to speculate whether the cited references might describe an ISDN line utilizing ISDN and ADSL over ISDN signaling technologies. Consequently, the cited references do not teach obtaining (transmitting) an ISDN telephone number that uniquely identifies an ISDN line that utilizes both ISDN and ADSL over the ISDN line.

As we explained with respect to claim 1 *supra*, the Examiner has failed to provide a sufficient explanation as to how one would have understood Li's and Fijolek's separate network links to be a single network link utilizing ADSL over ISDN and ISDN signaling technologies. Consequently, we are constrained by the record before us to find that the combination of the Li and Fijolek references does not collectively teach or suggest the disputed limitation of Appellants' claim 10. It follows that Appellants have persuaded us to find error in the Examiner's obviousness rejection of independent claim 10. Claims 11-13 are dependent on independent claim 10. Therefore, based on the record before us, we find that the Examiner err in finding the Li and Fijolek references would have collectively taught or suggested obtaining, using an ISDN line, an ISDN telephone number uniquely associated with the ISDN line, as recited in Appellants' claims 10-13. Accordingly, we reverse the Examiner's obviousness rejection of claims 10-13.

CONCLUSIONS OF LAW

Appellants have shown that the Examiner erred in rejecting claims 1-41 under 35 U.S.C. § 103(a).

DECISION

We reverse the Examiner's rejection of claims 1-41 under 35 U.S.C. § 103(a).

REVERSED

llw

Hickman Palermo Truong & Becker, LLP
2055 Gateway Place
Suite 550
San Jose, CA 95110